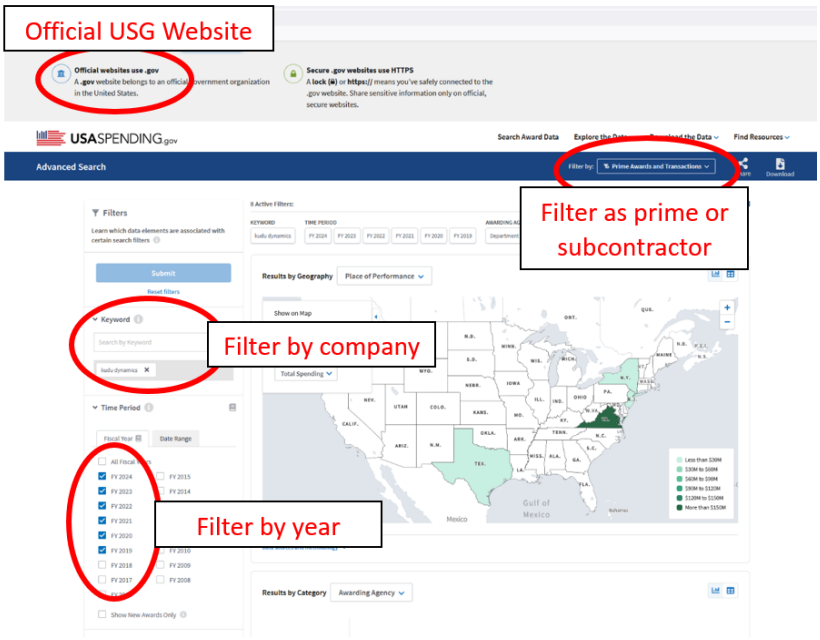
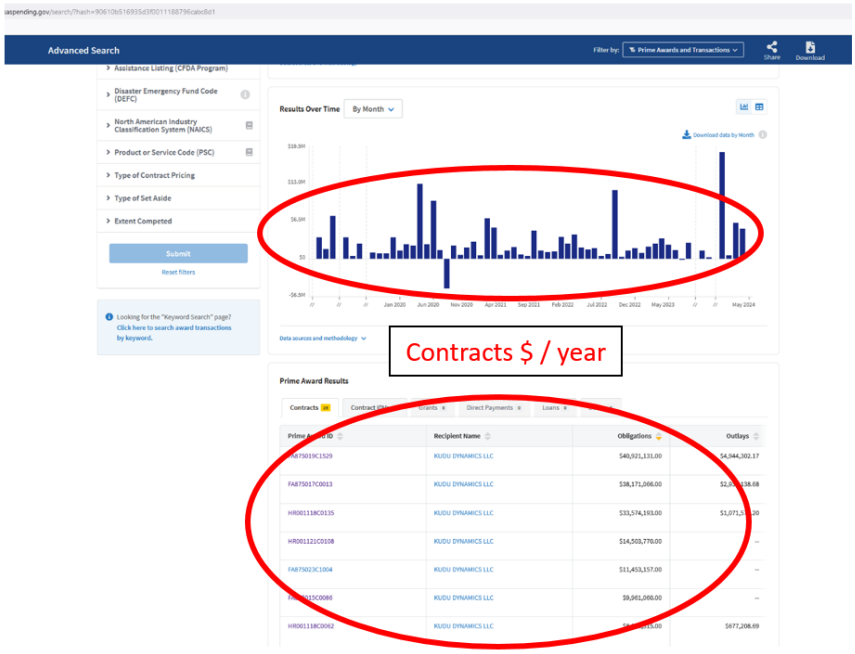
EXHIBIT 3 TO RESPONSE TO MOTION TO MOTION TO EXCLUDE EXPERT TESTIMONY

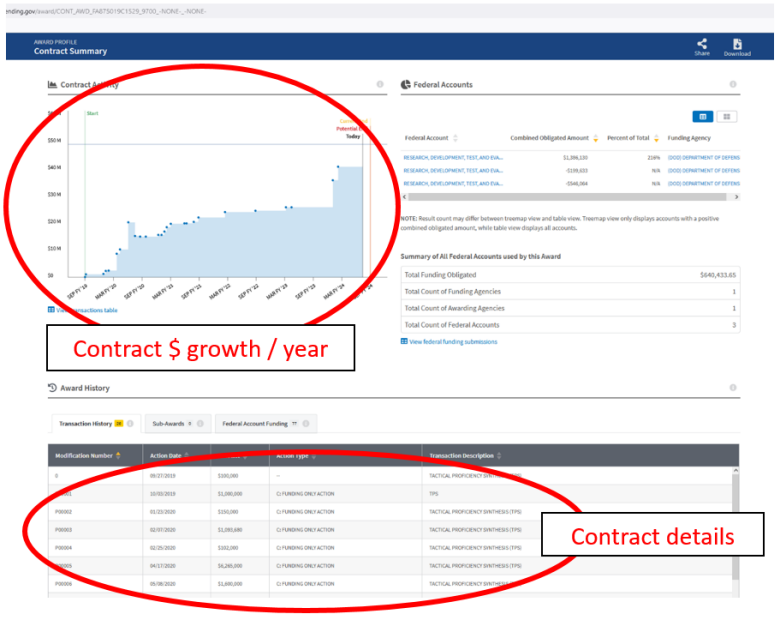
CyberAI Market Analysis

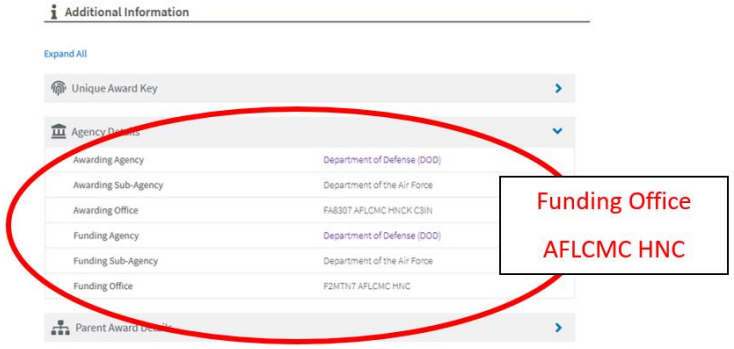
Introduction

A market analysis can be created using a United States Government (USG) website: usaspending.gov. In this example we will use Kudu Dynamics because they were a subcontractor on the same contract during my employment and consulting for Air Force Life Cycle Management Center (AFLCMC) HNCO. Using this website we can filter by company, prime contractor or sub-contractor, filter by government agency, filter by year, etc. The website provides the details of every contract awarded by the USG to that company, as well as the details of the contract, the awarding office (e.g., AFLCMC HNCO) the contract growth over time, and the type of work and deliverables of the contract, e.g., research and development on cybersecurity for $X dollars, for agency Y, under the contract name Z or classified code word Z. See the usaspending.gov screenshots provided below.









Using the contract name, we can further research the awarding government agency and the request for proposal (RFP) document that describes in detail what is required for a contract to be awarded, e.g., "Employ AI large language models to discover remote access capabilities or exploitation for a Windows 10 computer".

Most of our open-source intelligence (OSINT) gathering in this market analysis uses two government websites, https://sam.gov/search and https://www.usaspending.gov/search, after which a Google Search can be used to determine further contract details, e.g., the RFP. Every company in the United States is required to register on sam.gov so that they can receive a Cage Code and tracking number that enable them to do business with the USG. The USG then provides public documentation of all contracts awarded.

OSINT information on basic details of the company size, location, number of employees, etc., can be found from paid and free sources, e.g., https://www.crunchbase.com/organization/kudu-dynamics and https://www.linkedin.com/company/kudu-dynamics-llc/.

For reference, this method of OSINT gathering is the same method used by my colleague at Leidos, Padraig Maloney, Vice President of external business and investments (competitive business intelligence).

Kudu, Cynnovative, and Def-Logix had contracts the same time I was a consultant. Part of my job was to review their work for the AFLCMC HNCO. Their contract was canceled when my contract was canceled. You can see this cancellation reflected on usaspending.gov. Their contract cancellation and program cancellation was associated with my name not their name, so their companies survived, and continue to receive other contracts. I did not.

For this market analysis we will consider the following information:

- company name
- # of employees
- # of contracts and value in the last 5 years
- source of contracts

We will look at the following companies that are key players and founders in the field of CyberAI, most of whom I know personally and have worked with for +5 years (Note: CyberAI is a new field that did not formally exist on government contracts prior to 2019).

- CNF Technologies
- Def-Logix
- Kudu Dynamics
- Cynnovative
- Two Six Labs

This analysis will provide the "straight forward" funding lines. There are other methods used by the USG to fund companies and consultants. For example, my funding was filtered through AFCYBER to Air Force Research Laboratory (AFRL), then to GiTi using the ACT2 contract. I was not a performer on the ACT2 contract, but it was an easy way for the USG to provide funding through an existing contract and guide that funding to a specific individual as a "consultant" to the USG through another contract.

Case Studies

The following companies were selected because they work exclusively in Cyber, have started using AI in their offerings, and are now hiring AI and CyberAI researchers (as evidence that they are now doing CyberAI research). While these companies have many contracts as a sub-contractor, we limit our analysis to prime-contractor only contracts. If we include sub-contracts, the CyberAI portfolio of each company more than doubles in value. Similarly, these companies have contracts with many government agencies, so for this analysis we will only consider Department of Defense (DoD) contracts and predominately Air Force Cyber. We are providing the total cyber contracts value for a 5 year period FY2020 - FY2024, the total value of contracts awarded during this period is $713.85M, with an **average value of $28.5M per year** for each company.

Case Study 1: Kudu Dynamics

- # of employees = 112
- # of contracts and value in the last 5 years: 26 contracts and **$151.15M** (prime contractor)
- source of contracts: DoD
- notes: 20 contracts of $1.5M to $41M

Case Study 2: Cynnovative LLC

- # of employees = 20
- # of contracts and value in the last 5 years: 6 contracts and **$17.96M** (prime contractor)
- source of contracts: DoD
- notes: 3 contracts of $3.6M to $9.4M, example CyberAI job ad below

CYNNOVATIVE

CAPABILITIES \ CAREERS \ COMPANY \ BLOG \ CONTACT

AI RESEARCH SCIENTIST

COMPANY OVERVIEW

At Cynnovative, we leverage machine learning, computer science, and software engineering to address high-impact problems in the cyber domain, specifically those which are critical to U.S. national security. We primarily extend fundamental research to invent, design, develop, and deploy prototype solutions that support persistent problems in this domain.

JOB OVERVIEW

AI Research Scientists at Cynnovative drive innovation by conceiving, designing, and developing novel AI and machine learning algorithms to tackle complex cyber-related challenges. As an AI Research Scientist, you will advance the state-of-the-art in AI research, collaborating with cross-functional teams to integrate your findings into practical solutions that support U.S. national security.

This is a research-intensive role, requiring expertise in multiple areas of AI research, as well as the ability to read, understand, and leverage academic research across multiple domains to generate novel concepts and prototypes. You will have opportunities to publish research papers, collaborate with academia and industry partners, and contribute to the development of cutting-edge AI solutions.

RESPONSIBILITIES \ MAY INCLUDE

- Conduct original research in AI and machine learning, with a focus on cyber-related applications
- Serve as the principal investigator on research projects
- Develop novel algorithms and models that advance the state-of-the-art in AI
- Collaborate with data scientists and engineers to integrate research into larger systems
- Publish research papers and present at conferences
- Collaborate on composing proposals, white papers, and presentations for new and existing customers

Case Study 3: Two Six Labs

- # of employees = 75
- # of contracts and value in the last 5 years: 32 contracts and **$340.27** (prime contractor)
- source of contracts: DoD
- notes: 40 contracts of $1.1M to $105.5M

Case Study 4: CNF Technology

- # of employees = 150
- # of contracts and value in the last 5 years: 8 contracts and **$145.17** (prime contractor)
- source of contracts: DoD
- notes: 4 contracts of $3.8M to $113.9M

Case Study 5: Def-Logix LLC

- # of employees = 66
- # of contracts and value in the last 5 years: 5 contracts and **$59.3** (prime contractor)
- source of contracts: DoD
- notes: 4 contracts of $1M to $54.9M

Relevance of CyberAI Research

America has a problem, our national critical infrastructure is vulnerable to not only cyber-attacks, but advanced AI-enabled cyber-attacks from nation-state adversaries. According to a 2023 Harvard Business Review (HBR)[1]

- The 2017 Equifax hack affected 143 million Americans and cost the FTC $425 million.
- Ransomware attacks in America from 2018-2023 cost taxpayers $20.9 billion.
- The 2021 Colonial Pipeline ransomware attack affected 45% of all fuel availability on the East Coast.
- In the last few years, 41% of all cyber-attacks focused on small to medium businesses, while 59% focused on government and infrastructure.

For the last two decades I have worked for, and with customers in, the Intelligence Community (IC), the DoD and industry. While all of these customers want access to modern AI-enabled cybersecurity capabilities, they all have the same constraints limiting AI adoption:

1. **Constraint:** Most critical networks use legacy software and hardware, e.g., Windows XP running on Pentium II processors[2], and government agencies and corporations do not have sufficient funding to update their networks.
    - **Solution: Advanced AI-enabled cyber tools are needed that can operate on legacy systems**.
2. **Constraint:** Until recently, annual penetration testing was the minimum requirement for compliance with federal law. Now, advanced and more frequent penetration testing is required[3] for critical systems.
    - **Solution: Advanced tools are needed to automate daily testing that replicate advanced nation-state adversaries**.
3. **Constraint:** Presently, due to the popularity of ChatGPT and the subsequent demand for compute, GPUs from AMD and Nvidia (sufficiently advanced to handle the modern complex AI models) are backordered 2 years, and even prior generation GPUs are available at a premium on the grey-market. Compounding this issue is the lack of availability of cloud compute (servers of GPUs for training and deploying AI models), e.g., Amazon AWS, Google Cloud, Microsoft Cloud, GovCloud, or IC GovCloud.
    - **Solution: Fundamental advancement in AI algorithms is needed to run on smaller existing legacy hardware** (e.g., micro-processors in PLCs on a SCADA networks), **and run more efficiently, thereby reducing time, energy, and financial costs**.

[1] https://hbr.org/2023/04/what-business-needs-to-know-about-the-new-u-s-cybersecurity-strategy
[2] Based on information from FAA, CISA, DHS and US Air Force.
[3] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-legislation-preparing-for-increased-reporting-and-transparency

Market Analysis for CyberAI Tools

Given the relevance of CyberAI research, there are many factors that position CyberAI tools to capture an emerging and necessary market segment. Here are a few examples:

- According to McKinsey & Company[4], Industrial Manufacturing, Energy, and Government (state and local) are the areas of greatest concern for cyber-attacks that affect large populations in the United States.
- In August 2023, the Biden Administration launched the AI Cyber Challenge[5] which was followed by an Executive Order[6] in October 2023.
- In 2022 the US Congress approved an $858 billion defense spending budget that includes Cyber AI[7] for FY23, which was again augmented for FY24.
- In 2023, CISA approved $1.7 billion in funding for Cyber AI[8].
- In 2023, US Congress approved a bill to support hiring and education of federal employees in cyber and AI[9].

Clearly there is a growing need for CyberAI, and US government is finally taking AI-enabled cyber-attacks seriously, and is ready to spend money backed by legislative cyber and AI compliance initiatives.

Clearly the issues are scale, cost, number of Americans affected, and the consequences affecting infrastructure. HBR also notes the necessity for better penetration testing (use offense tools to find gaps and improve defense tools) by hiring "ethical hackers" and "red teams", as well as improved technical readiness and more capable cybersecurity systems.

Finally, while many customers have reported to that they do not have time or money for better defenses, or that they do not have a "compliance reason", McKinsey[10] notes the Cyber Incident Reporting for Critical Infrastructure Act signed into law March 2022 requires increased reporting, transparency, and compliance by the government and commercial sector in critical infrastructure.

Opinion

Based on my opinion and as a subject matter expert in AI and Cyber, the average CyberAI contracts value for small businesses working for the DoD over the last 5 year period is $142.5M; this is based on the evidence provided above, with data gathered from a government website. Based on the recent advancements in both AI and Cyber, e.g., ChatGPT and the Executive orders referenced above for both AI and Cyber, the CyberAI contracts value is surely to increase many fold in the next 5 years.

---

[4] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/critical-infrastructure-companies-and-the-global-cybersecurity-threat

[5] https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/09/biden-harris-administration-launches-artificial-intelligence-cyber-challenge-to-protect-americas-critical-software/

[6] https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

[7] https://www.appropriations.senate.gov/imo/media/doc/JRQ121922.PDF

[8] https://www.appropriations.senate.gov/imo/media/doc/FY23%20Omnibus%20Full%20Summary.pdf

[9] https://oversight.house.gov/wp-content/uploads/2023/07/HR4502.Cyber_Education_xml.Mace_-1.pdf

[10] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-legislation-preparing-for-increased-reporting-and-transparency

Signed,

Paul F. Roysdon, Ph.D.